

日 本 国 特 許 庁
JAPAN PATENT OFFICE

23. 4. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 2 月 2 6 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 4 3 2 4 4 7
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 4 3 2 4 4 7]

REC'D 01 JUL 2004	
WIPO	PCT

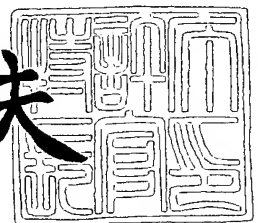
出 願 人 三 菱 電 機 株 式 会 社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 6 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 548698JP01
【提出日】 平成15年12月26日
【あて先】 特許庁長官殿
【国際特許分類】 G09F 15/00
【発明者】
 【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
 【氏名】 大越 丈弘
【発明者】
 【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
 【氏名】 山田 敬喜
【発明者】
 【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
 【氏名】 牧田 覚
【特許出願人】
 【識別番号】 000006013
 【氏名又は名称】 三菱電機株式会社
【代理人】
 【識別番号】 100099461
 【弁理士】
 【氏名又は名称】 溝井 章司
【手数料の表示】
 【予納台帳番号】 056177
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、

上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持していない場合に新たな認証用鍵を生成し、上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持している場合で上記認証処理部による上記被認証装置との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部とを備え、

上記認証処理部は、上記更新鍵生成部により生成された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする認証装置。

【請求項 2】

上記認証装置は、さらに、

被認証装置から所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部を備え、

上記更新鍵生成部は、上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記新たな認証用鍵を生成し、

上記認証装置は、さらに、

上記更新鍵生成部により生成された新たな認証用鍵を被認証装置に送信する送信部を備え、

上記認証処理部は、上記送信部により送信された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする請求項 1 記載の認証装置。

【請求項 3】

所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する記憶部と、

認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、

上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいた新たな認証用鍵を受信する受信部とを備え、

上記認証処理部は、上記受信部により受信された新たな認証用鍵を用いて上記認証装置との間での認証処理を再度おこなうことを特徴とする被認証装置。

【請求項 4】

上記受信部は、上記認証処理部による上記認証装置との間での認証処理が失敗した場合に、上記認証装置から所定の情報を受信し、

上記送信部は、上記受信部により所定の情報が受信された場合に、上記記憶部により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを認証装置に送信することを特徴とする請求項 3 記載の被認証装置。

【請求項 5】

所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信する第 1 の送信工程と、

上記第 1 の送信工程により上記認証装置から送信された所定の情報を上記被認証装置が受信する第 1 の受信工程と、

上記第 1 の受信工程により上記所定の情報が受信された後、上記被認証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信する第 2 の送信工程と、

上記第 2 の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置が受信する第 2 の受信工程と、

上記第 2 の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子

とに基づいて、上記認証装置が新たな認証用鍵を生成する生成工程と、
上記生成工程により生成された新たな認証用鍵を被認証装置に送信する第 3 の送信工程と、
上記第 3 の送信工程により送信された新たな認証用鍵を上記被認証装置が受信する第 3 の受信工程と、
上記第 3 の受信工程により受信された新たな認証用鍵を、上記被認証装置と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこなう鍵更新工程と、
更新確認データを生成して上記認証装置へ送信する工程と、
更新確認データを受信し、確認する工程と
を備えたことを特徴とする鍵更新方法。

【書類名】 明細書

【発明の名称】 認証装置及び被認証装置及び鍵更新方法

【技術分野】

【0001】

本発明は、認証装置、被認証装置、或いは両者の鍵更新方法に関する。特に、ETC（ノンストップ自動料金支払いシステム）やドライブスルー等、無線通信機能を有する移動体及び移動体通信システムに関する。

【背景技術】

【0002】

利用者があるサービスを受けるとき、サービスを受けられる正当な利用者であるか本人確認（認証）が行われる。その際、鍵なし・期限切れ等の理由により認証に失敗するとサービスを受けることができない。

【特許文献1】 特開 2003-196240 号公報

【特許文献2】 特開平 11-274999 号公報

【特許文献3】 特開 2000-138674 号公報

【特許文献4】 特開 2000-196588 号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

利用者は、鍵の更新等正当な利用者であるための手続きを怠ると、たとえ正当な利用者であっても（不正を行う意図はなくとも）、サービスを受けることができなくなるといった問題があった。

【0004】

また、上記特許文献1に記載の技術では、テンポラリーで認証が許可されてしまうため、過去に認証に成功していれば、その後何度でも認証されてしまい、認証装置にアクセス可能となることからセキュリティホールになりかねないといった問題があった。

【0005】

また、上記特許文献2～4に記載の技術では、双方が保持している鍵の中から、使用鍵を決定しているに過ぎず、鍵更新をおこなうことができないといった問題があった。

【0006】

本発明は、鍵更新をおこなうことで更新された鍵により正当な利用者に対しては、サービスを提供し、サービスの可用性及び利用者の利便性を向上させることを目的とする。

【課題を解決するための手段】

【0007】

この発明に係る認証装置は、認証用鍵を用いて被認証装置との間で認証処理をおこなう認証処理部と、

上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持していない場合に新たな認証用鍵を生成し、上記認証処理部による認証処理に用いる認証用鍵を上記被認証装置が保持している場合で上記認証処理部による上記被認証装置との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部とを備え、

上記認証処理部は、上記更新鍵生成部により生成された新たな認証用鍵を用いて上記被認証装置との間での認証処理を再度おこなうことを特徴とする。

【発明の効果】

【0008】

本発明によれば、鍵なし・期限切れ等の場合であっても鍵の更新をおこなうことができ、その後に正当な利用者がサービスの提供を受けることができ、本発明を利用するシステムのサービスの可用性及び利用者の利便性を向上させることができる。

【発明を実施するための最良の形態】

【0009】

実施の形態 1.

以下に説明するように、被認証装置と認証装置との間での認証時、被認証装置が鍵なし又は被認証装置が有する鍵が有効期限切れであっても、認証失敗とするのではなく、鍵更新手段により鍵更新を実施し、その後、認証を行うものである。

【0010】

図1は、実施の形態1における認証システムの構成を示す図である。

【0011】

図1において、認証システムは、認証装置となる通信装置100と被認証装置となる通信装置200とを備えている。通信装置100は、アンテナ101、通信処理部110、記憶部120、制御部130、更新処理部196、認証処理部197を備えている。通信処理部110は、受信部111、送信部112を有している。更新処理部196は、暗号処理部140、乱数生成部150、更新鍵生成部160、個別鍵生成部170、一時鍵生成部180、更新用データ生成部190、更新確認データチェック部195を有している。通信装置200は、アンテナ201、通信処理部210、記憶部220、制御部230、更新処理部296、認証処理部297を備えている。通信処理部210は、受信部211、送信部212を有している。更新処理部296は、暗号処理部240、乱数生成部250、一時鍵生成部280、更新用データチェック部290、更新確認データ生成部295を有している。実施の形態1では、通信装置100と通信装置200とは、アンテナ101、201を介して無線通信する場合を説明するが、これに限るものではなく有線通信であっても構わない。例えば、ETC（料金自動収集）、ドライブスルー等において、通信装置100は、店舗側の路側機として、通信装置200は、自動車側の車載機として構成される。

【0012】

図2は、実施の形態1における認証システムの概念を示す図である。

【0013】

例えば、ETC、ドライブスルー等において、通信装置100は、店舗側の路側機として、通信装置200は、自動車側の車載機として構成される場合、ETC、ドライブスルー等によるサービス提供において、店舗側の路側機は、起動後、認証処理を実施する状態で、利用者（自動車）の来店（通過）を待ち続ける。

【0014】

利用者が来店すると、路側機は自動車に設置された車載機に対して認証要求を送信する。

【0015】

車載機は路側機の指示にしたがって必要な情報を路側機に送信する。

【0016】

路側機は、車載機から受け取った情報が古い或いは鍵がないと判断した場合、鍵更新の状態となり、車載機に対して鍵更新要求を実施する。

【0017】

車載機は、路側機の指示にしたがって鍵更新を実施する。

【0018】

鍵更新終了後、路側機は認証状態となり、車載機に対して認証処理を実施する。

【0019】

言い換えれば、本実施の形態1における認証システム或いは認証方式は、鍵更新手段を備えている。そして、認証処理と更新処理が分離している。認証処理中は、更新処理はされない。

【0020】

そして、鍵情報が古い又はない場合、鍵更新を実施してから認証処理を実施する。すなわち、初期時（鍵情報がなくとき）、鍵更新処理を実施する。或いは、通常運用時は認証処理を実施して、認証に用いる鍵情報が古い場合、鍵更新処理を実施する。

【0021】

図3は、実施の形態1における鍵更新方法の手順を示すフローチャート図である。

【0022】

記憶部120は、所定のアルゴリズム識別子と所定の暗号鍵識別子と、上記所定のアルゴリズム識別子に対応するアルゴリズムを記憶している。

【0023】

記憶部220は、所定のアルゴリズム識別子と所定の暗号鍵識別子と、上記所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵と装置固有番号とを記憶している。また、上記記憶部220は、古くなった或いは使用期限が過ぎた認証用鍵及びその認証用鍵の識別子を記憶している。或いは、記憶部220は、認証用鍵を記憶していない場合であってもよい。ここで、所定の暗号鍵識別子は、鍵更新専用の鍵の識別子（更新用識別子）である。所定の暗号鍵識別子に対応する暗号鍵は、鍵更新専用鍵である。この鍵更新専用の鍵の識別子及び鍵更新専用鍵は、初期時（例えば装置の出荷時）における新規鍵生成に伴う鍵更新処理、或いは通常運用時に発生した鍵更新処理において、通信装置100、200間で互いに共有できる認証用鍵が存在しない緊急時における別の新たな鍵生成に伴う鍵更新処理のいずれかの場合に用いる。認証処理に用いることはない。

【0024】

まず、認証処理部197は、被認証装置となる通信装置200との間で認証処理をおこなう。言い換えれば、認証処理部297は、認証装置となる通信装置100との間で認証処理をおこなう。認証処理の際、認証用鍵を用いておこなう。ここで、記憶部220が、古くなった或いは使用期限が過ぎた認証用鍵を記憶している場合、或いは、記憶部220が、認証用鍵を記憶していない場合、認証用鍵が使用できないので、ここでの認証処理は失敗に終わることになる。

【0025】

S（ステップ）201において、乱数生成工程として、上記認証処理が失敗に終わると、乱数生成部150は、乱数1を生成する。

【0026】

S202において、送信工程として、送信部112は、乱数生成部150により生成された乱数1（所定の情報の一例である）を通信情報1として通信装置200に送信する。通信装置100は、乱数1を通信情報1として通信装置200に送信することで、認証処理から鍵更新処理に移行したことを通信装置200へ知らせることになる。

【0027】

S203において、受信工程として、受信部211は、送信部112により送信された乱数1を通信情報1として受信する。通信装置200では、受信部211が、乱数1を受信したことにより、通信装置100より鍵更新が要求されたと判断する。

【0028】

S204において、認証処理工程の一部として、乱数生成部250は、乱数2を生成する。

【0029】

S205において、送信工程として、送信部212は、上記記憶部220により記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子と装置固有番号と、乱数生成部250により生成された乱数2とを通信情報2として認証装置である通信装置200に送信する。存在する場合には、古くなった或いは使用期限が過ぎた認証用鍵の識別子と対応するアルゴリズムの識別子とを一緒に送信する。ここで、1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組みとしてプロファイルとして表し、通信情報2は、乱数2と装置固有番号と組数分のプロファイル数とプロファイル数分の各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とをデータとして有している。さらに、ここでは、各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とを対応させたデータとしている。言い換えれば、上記送信部212は、上記記憶部220により1つのア

ルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置となる通信装置100に送信する。

【0030】

S206において、受信工程として、受信部111は、被認証装置となる通信装置200から、乱数2と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも1つのプロファイル識別子と少なくとも1つのプロファイル識別子の各プロファイル識別子に対応した少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを有する通信情報2を受信する。

【0031】

S207において、生成工程として、更新鍵生成部160は、上記受信部111により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から上記鍵更新専用の鍵の識別子である所定の暗号鍵識別子と所定の暗号鍵識別子に対応する上記所定のアルゴリズム識別子とを選択する。そして、更新鍵生成部160は、上記受信部111により受信された装置固有番号等とたとえばハッシュ値等を用いて更新鍵となる新たな認証用鍵を生成する。言い換えれば、更新鍵生成部160は、上記受信部111により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記認証処理部197による認証処理に用いる認証用鍵を上記被認証装置となる通信装置200が保持していない場合に新たな認証用鍵を生成し、上記認証処理部197による認証処理に用いる認証用鍵を上記被認証装置となる通信装置200が保持している場合で上記認証処理部197による上記被認証装置となる通信装置200との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する。

【0032】

S208において、個別鍵生成工程として、個別鍵生成部170は、上記更新鍵生成部160により選択された所定の暗号鍵識別子に対応する暗号鍵となる通信装置200が有している鍵更新専用鍵となる個別鍵を更新鍵生成部160と同様の方法で生成する。

【0033】

S209において、一時鍵生成工程として、一時鍵生成部180は、上記更新鍵生成部160により選択された所定のアルゴリズム識別子に対応するアルゴリズムを用いて所定の暗号鍵識別子に対応する暗号鍵となる個別鍵生成部170により生成された個別鍵で乱数1, 2を暗号処理部140を用いて暗号化し、鍵更新処理用暗号鍵の一例となる一時鍵を生成する。

【0034】

S210において、更新用データ生成工程として、更新用データ生成部190は、乱数2のすべて或いは一部と、更新鍵となる新たな認証用鍵とを暗号処理部140により一時鍵生成部180により生成された一時鍵で暗号化することにより更新用データを生成する。

【0035】

S211において、送信工程として、送信部112は、上記更新鍵生成部160により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のプロファイル識別子と更新用データ生成部190により生成された更新用データとを通信情報3として上記被認証装置となる通信装置200に送信する。

【0036】

S212において、受信工程として、受信部211は、上記認証装置となる通信装置100から上記送信部212により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定の暗号鍵識別子とに対応するプロファイル識別子と更新用データとを通信情報3として受信する。言い換えれば、上記受信部211は、上記認証装置となる通信装置100から上記送信部212により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいた新たな認証用鍵を受信する。

【0037】

S213において、確認工程として、暗号処理部240は、受信部211により受信されたプロファイル識別子を確認し、プロファイル識別子に対応する所定の暗号鍵識別子と所定のアルゴリズム識別子とを確認する。

【0038】

S214において、一時鍵生成工程として、一時鍵生成部280は、受信部211により受信され、暗号処理部240により確認された所定のアルゴリズム識別子に対応するアルゴリズムを用いて、記憶部220に記憶された個別鍵で乱数1, 2を暗号処理部240を用いて暗号化し、更新処理用暗号鍵の一例となる上記一時鍵を生成する。以上により通信装置100, 200間で同じ一時鍵という鍵共有ができたことになる。なお、この実施形態では、一時鍵生成部180, 280が一時鍵生成の際、個別鍵で暗号化したが、認証装置と被認証装置とが同じ処理を実施すればよいため、復号してもよい。

【0039】

S215において、更新用データチェック工程として、更新用データチェック部290は、受信部211により通信情報3として受信された暗号化されている更新用データを一時鍵生成部280により生成された一時鍵により暗号処理部240を用いて復号する。

【0040】

S216において、鍵更新工程の一部として、更新用データチェック部290は、復号した更新用データのデータが、通信装置200が通信装置100に送信した乱数2のすべて或いは一部であるかどうかを確認する。復号した更新用データのデータが乱数2のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置100との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置100, 200間での認証処理の一方が成功したことを意味する。そして、更新用データチェック部290は、復号することによって得られた上記受信部211により受信された新たな認証用鍵を、上記通信装置100と通信装置200との間での認証処理をおこなうための更新鍵として鍵更新をおこなう。更新鍵は、記憶部220に記憶される。

【0041】

S217において、更新確認データ生成工程として、更新確認データ生成部295は、乱数1のすべて或いは一部を暗号処理部240により一時鍵生成部280により生成された一時鍵で暗号化することにより更新確認データを生成する。

【0042】

S218において、送信工程として、送信部212は、更新確認データ生成部295により生成された更新確認データを通信情報4として通信装置100に送信する。

【0043】

S219において、受信工程として、受信部111は、通信装置200から更新確認データを通信情報4として受信する。

【0044】

S220において、更新確認データチェック工程として、更新確認データチェック部195は、受信部111により通信情報4として受信された暗号化されている更新確認データを一時鍵生成部180により生成された一時鍵により暗号処理部140を用いて復号する。

【0045】

S221において、更新確認データチェック工程として、更新確認データチェック部195は、復号した更新確認データのデータが、通信装置100が通信装置200に送信した乱数1のすべて或いは一部であるかどうかを確認する。復号した更新確認データのデータが乱数1のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置200との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置100, 200間での認証処理の他方が成功したことを意味する。

【0046】

以上により、通信装置100, 200間での鍵更新処理が終了し、その後、上記認証処理部197は、上記更新鍵生成部160により生成された新たな認証用鍵を用いて上記被

認証装置となる通信装置 200 との間での認証処理を再度おこなう。言い換えれば、上記認証処理部 297 は、上記受信部 211 により受信された新たな認証用鍵を用いて上記認証装置となる通信装置 100 との間での認証処理を再度おこなう。

【0047】

図 4 は、通信情報 1 のフレームの一例を示す図である。

【0048】

図 4 において、通信情報 1 は、ヘッダと乱数 1 データを有している。

【0049】

図 5 は、通信情報 2 のフレームの一例を示す図である。

【0050】

図 5 において、通信情報 2 は、ヘッダと乱数 2 データと装置固有番号（装置固有 No.）とプロファイル数（Profile 数）と各プロファイルを識別するプロファイル識別子としての Profile 1, … Profile n と、各プロファイル識別子に対応するアルゴリズム識別子（アルゴリズム ID）と暗号鍵識別子（鍵 ID）とを有している。プロファイルの最終番号に鍵更新専用の鍵の識別子（更新用識別子）と更新用識別子に対応するアルゴリズム識別子が記載されている。図 5 では、各プロファイル識別子と各プロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

【0051】

図 6 は、通信情報 3 のフレームの一例を示す図である。

【0052】

図 6 において、通信情報 3 は、ヘッダと選択された所定のプロファイルを識別する所定のプロファイル識別子としての Profile n と、所定のプロファイル識別子に対応するアルゴリズム識別子（アルゴリズム ID）と暗号鍵識別子（鍵 ID）と更新用データとを有している。図 5 では、所定のプロファイル識別子と所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

【0053】

図 7 は、通信情報 4 のフレームの一例を示す図である。

【0054】

図 7 において、通信情報 4 は、ヘッダと更新確認データとを有している。

【0055】

ここで、制御部 130 は、通信装置 100 の各部を制御する。また、制御部 230 は、通信装置 200 の各部を制御する。また、記憶部 120 は、通信装置 100 の各部で行なわれる処理中に生じるデータを記憶する。また、記憶部 220 は、通信装置 200 の各部で行なわれる処理中に生じるデータを記憶する。

【0056】

以上のように、本実施の形態 1 における鍵更新方法は、所定のアルゴリズム識別子と所定の暗号鍵識別子とを記憶する被認証装置と、認証装置との間で認証用鍵を用いておこなう認証処理が失敗した場合に、上記認証装置から所定の情報を上記被認証装置に送信する第 1 の送信工程と、上記第 1 の送信工程により上記認証装置から送信された所定の情報を上記被認証装置が受信する第 1 の受信工程と、上記第 1 の受信工程により上記所定の情報が受信された後、上記被認証装置から上記記憶された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置に送信する第 2 の送信工程と、上記第 2 の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置が受信する第 2 の受信工程と、上記第 2 の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて、上記認証装置が新たな認証用鍵を生成する生成工程と、上記生成工程により生成された新たな認証用鍵を被認証装置に送信する第 3 の送信工程と、上記第 3 の送信工程により送信された新たな認証用鍵を上記被認証装置が受信する第 3 の受信工程と、上記第 3 の受信工程により受信された新たな認証用鍵を、上記被認証装置

と認証装置との間での認証処理をおこなうための更新鍵として鍵更新をおこなう鍵更新工程と、更新確認データを生成して上記認証装置へ送信する工程と、更新確認データを受信し、確認する工程とを備えている。

【0057】

また、例えば、ETC、ドライブスルー等において、通信装置100は、店舗側の路側機として、通信装置200は、自動車側の車載機として構成される場合、以上のように、この認証方式を実施する車載機は、路側機からの指示に従って鍵更新へ状態が切り替わる（鍵更新を実施する）。そして、車載機が自身の判断により鍵更新へ状態が切り替わったり、鍵更新を要求することはない。また、この認証方式を実施する路側機は、車載機に対して鍵情報を要求及びチェックし、必要であれば鍵更新を車載機に指示する。すなわち、路側機主導で処理が行なわれる。

【0058】

また、ここでは、一例として、ETC、ドライブスルー等での自動車（車載機）と路側機（店舗システム）とに適用し、想定したが、通信装置は限定するものではない。例えば、基地局と携帯電話、無線LAN（基地局とパソコン）、R/W（リーダー/ライター）とRF Tag（電子タグ）といった固定局と移動局とにおける通信はもちろんのこと、モバイルとモバイルの通信等にも適用できる。

【0059】

以上のように、本実施の形態によれば、鍵なし・期限切れ等の場合であっても鍵の更新をおこなうことができ、その後に正当な利用者がサービスの提供を受けることができ、本発明を利用するシステムのサービスの可用性及び利用者の利便性を向上させることができる。

【0060】

また、本実施の形態によれば、さらに、セットアップ作業が不要となる。具体的には、例えば、車載機の出荷時及び店舗にて自動車に設置時、暗号通信に用いる鍵等車載機固有情報のセットアップが不要となる。そのため、製造においては同一の車載機を生産することができ生産効率が向上する。車載機固有の情報は、システムのセキュリティを維持するために重要なものであるため、セットアップ時の固有情報の取得は登録・作業者の限定といった細かな制限事項が発生する。しかし、セットアップ作業が不要なためどの業者でも設置でき流通コスト及び作業が軽減される。

【0061】

実施の形態2.

図8は、実施の形態2における鍵更新処理に至るまでの手順を示すフローチャート図である。

【0062】

S801において、認証処理部197は、被認証装置となる通信装置200との間で認証処理をおこなう。言い換えれば、認証処理部297は、認証装置となる通信装置100との間で認証処理をおこなう。認証処理の際、認証用鍵を用いておこなう。ここで、記憶部220が、古くなった或いは使用期限が過ぎた認証用鍵を記憶している場合、或いは、記憶部220が、認証用鍵を記憶していない場合、認証用鍵が使用できないので、ここでの認証処理は失敗に終わることになる。

【0063】

S802において、送信部112は、認証処理が失敗に終わったことを示す失敗データを通信装置200に送信する。

【0064】

S803において、受信部211は、通信装置100より失敗データを受信する。

【0065】

S804において、送信部212は、失敗データを受信したことを示す確認データ（Ack）を通信装置100に送信（返信）する。

【0066】

S805において、通信装置100は、図3に示す鍵更新方法による鍵更新処理を開始する。

【0067】

実施の形態1では、認証処理部197が、認証処理が失敗に終わったと判断した場合に、直ちに図3に示す鍵更新方法による鍵更新処理を開始するが、図8に示すように、認証処理が失敗に終わったことを通信装置100、200間で確認した後に鍵更新方法による鍵更新処理を開始するようにしてもよい。

【0068】

図9は、ハードウェア構成図である。

【0069】

以上の説明において、各実施の形態の説明において「～部」として説明したものを、一部或いはすべてコンピュータで動作可能なプログラムにより構成する場合、図9に示すように、通信装置100、200は、プログラムを実行するCPU(Central Processing Unit)37を備えている。CPU37は、内蔵された、或いはバス38を介してRAM(Random Access Memory)40(記憶装置、記憶部の一例である)、外部と通信可能な通信ポート44に接続されている。また、図9に示すように、ROM(Read Only Memory)39、磁気ディスク装置46等の記憶装置に接続されていても構わない。

【0070】

プログラムにより構成する場合、図9におけるプログラム群49には、各実施の形態の説明において「～部」として説明したものにより実行されるプログラムが記憶されている。プログラム群49は、上記記憶装置に記憶されている。プログラム群49は、CPU37、OS47等により実行される。記憶装置は、各処理の結果を記憶する。

【0071】

また、各実施の形態の説明において「～部」として説明したものは、ROM39に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

【0072】

また、上記各実施の形態を実施させるプログラムは、FD(Flexible Disk)、光ディスク、CD(コンパクトディスク)、MD(ミニディスク)、DVD(Digital Versatile Disk)等のその他の記録媒体による記録装置を用いて記憶されても構わない。係る場合には、図9に示すように、FDD(Flexible Disk Drive)45、コンパクトディスク装置(CDD)86等を備える。

【産業上の利用可能性】

【0073】

このような通信装置100、200は、ETC、ドライブスルー等における店舗側の路側機と自動車側の車載機に限らず、携帯電話等の移動体通信装置間、有線の通信装置間、或いは基地局を経由した有線と無線の通信装置間等における認証装置、被認証装置として、使用することができる。

【図面の簡単な説明】

【0074】

【図1】実施の形態1における認証システムの構成を示す図である。

【図2】実施の形態1における認証システムの概念を示す図である。

【図3】実施の形態1における鍵更新方法の手順を示すフローチャート図である。

【図4】通信情報1のフレームの一例を示す図である。

【図5】通信情報2のフレームの一例を示す図である。

【図6】通信情報3のフレームの一例を示す図である。

【図7】通信情報4のフレームの一例を示す図である。

【図8】実施の形態2における鍵更新処理に至るまでの手順を示すフローチャート図

である。

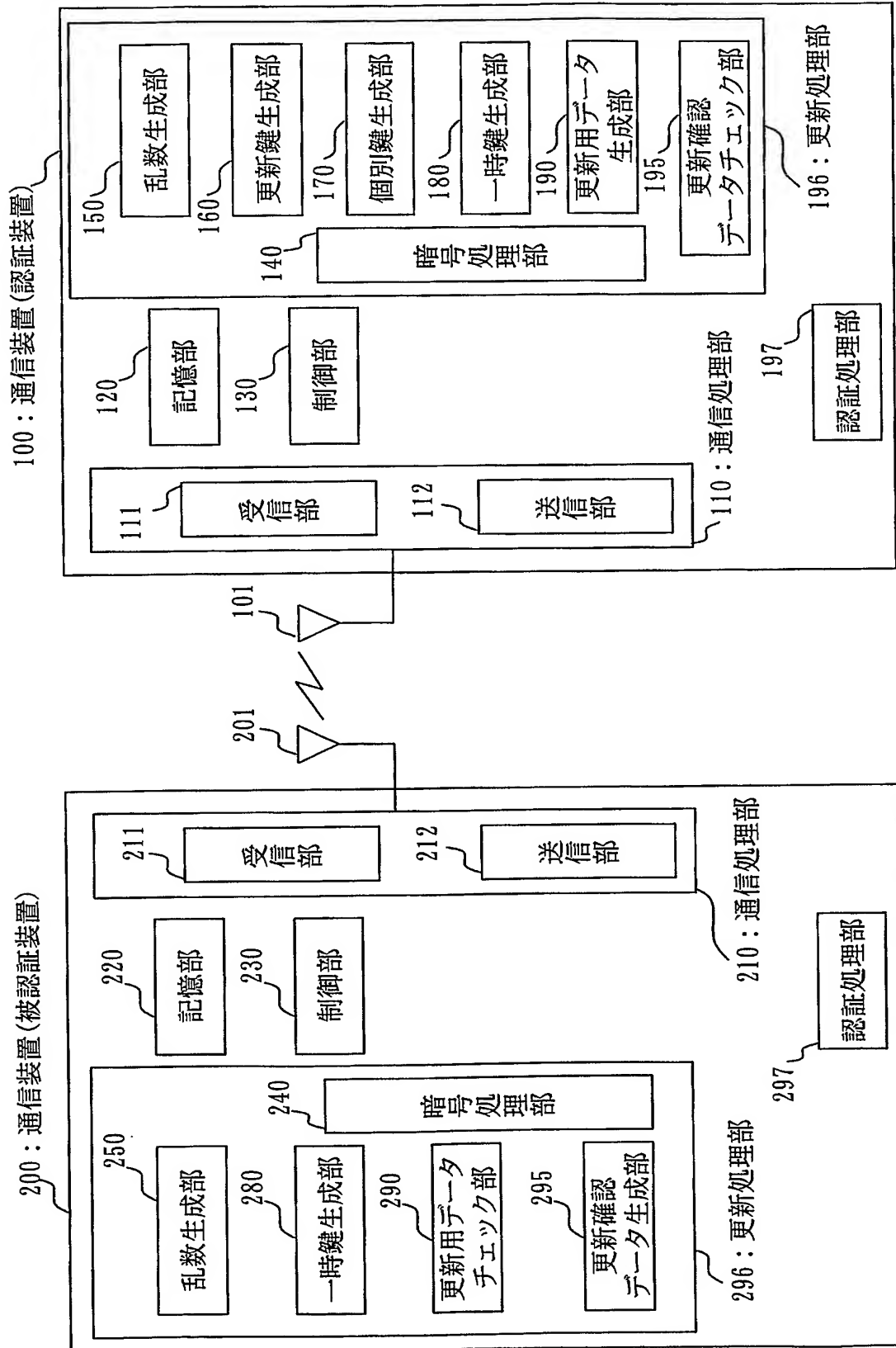
【図9】ハードウェア構成図である。

【符号の説明】

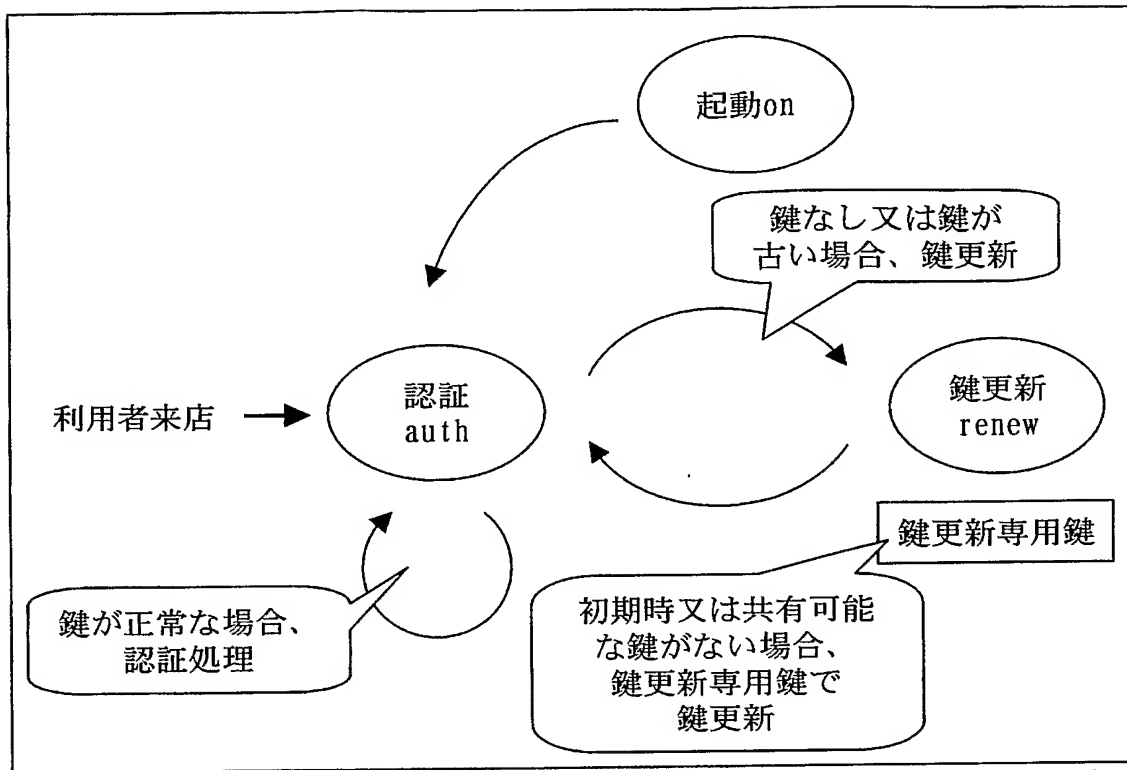
【0075】

37 CPU、38 バス、39 ROM、40 RAM、44 通信ポート、45 FDD、46 磁気ディスク装置、47 OS、49 プログラム群、86 CDD、100 通信装置、101 アンテナ、110 通信処理部、111 受信部、112 送信部、120 記憶部、130 制御部、140 暗号処理部、150 乱数生成部、160 更新鍵生成部、170 個別鍵生成部、180 一時鍵生成部、190 更新用データ生成部、195 更新確認データチェック部、196 更新処理部、197 認証処理部、200 通信装置、201 アンテナ、210 通信処理部、211 受信部、212 送信部、220 記憶部、230 制御部、240 暗号処理部、250 乱数生成部、280 一時鍵生成部、290 更新用データチェック部、295 更新確認データ生成部、296 更新処理部、297 認証処理部。

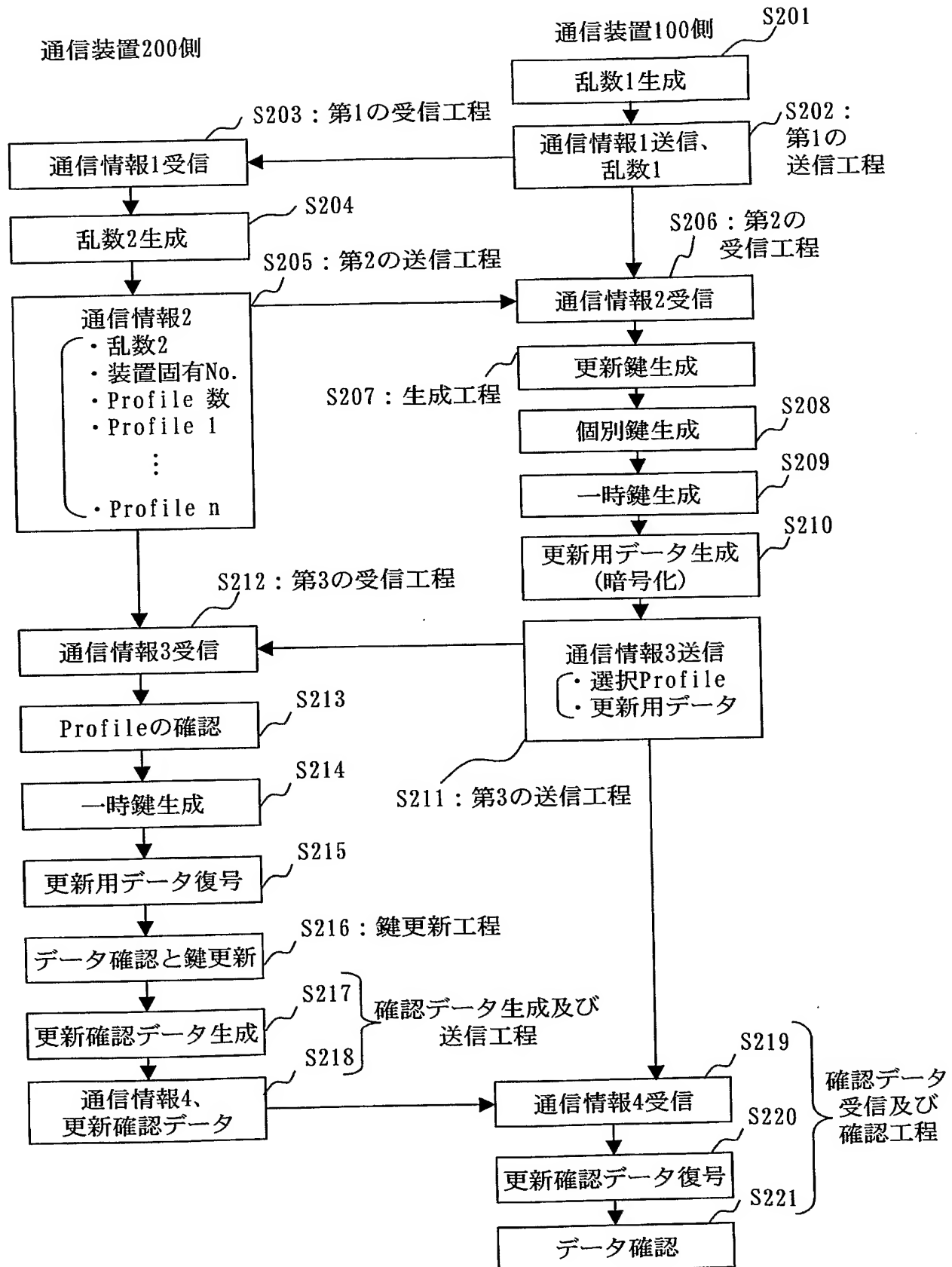
【書類名】 図面
【図 1】



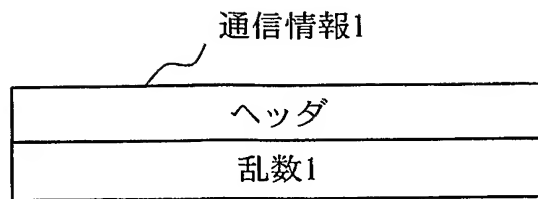
【図 2】



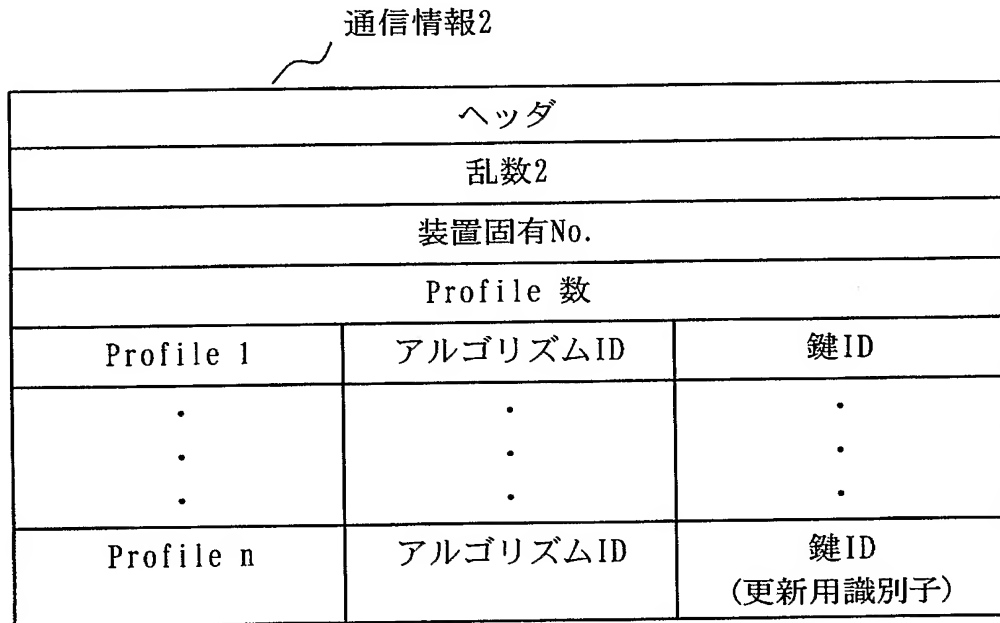
【図 3】



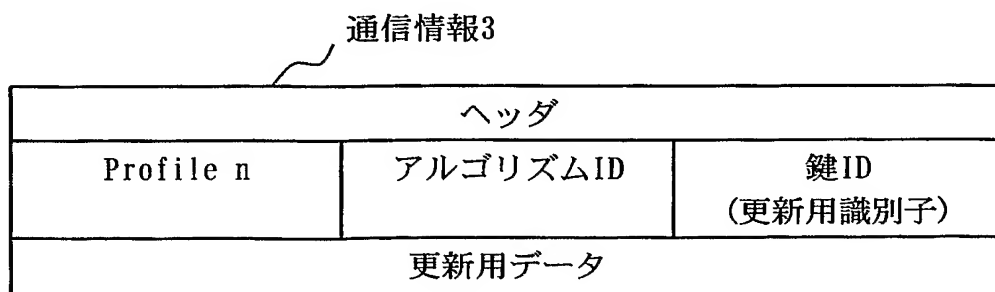
【図 4】



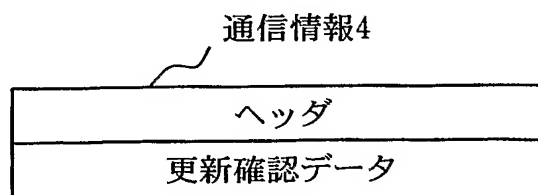
【図 5】



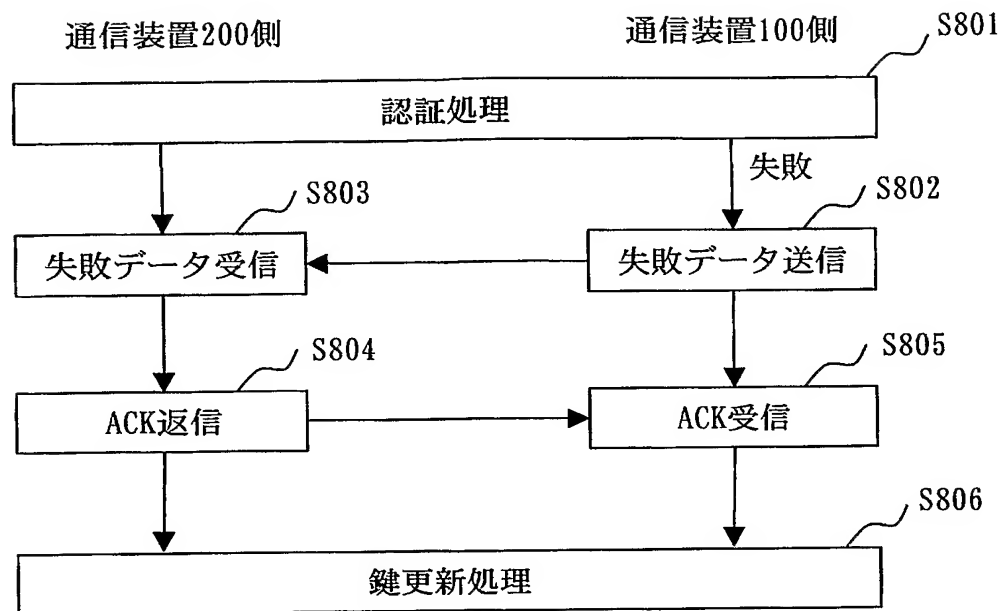
【図 6】



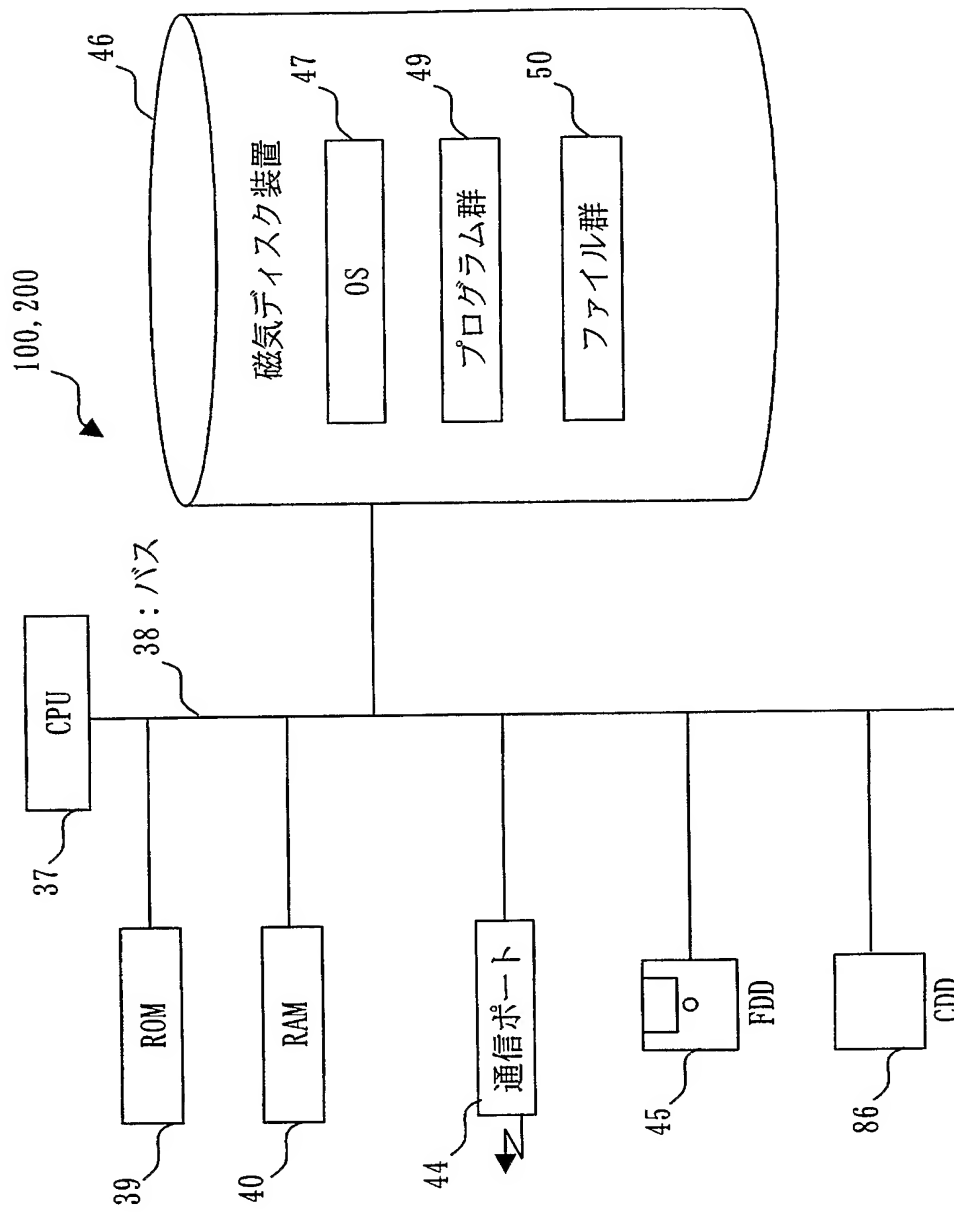
【図 7】



【図 8】



【図 9】



【書類名】 要約書**【要約】**

【課題】 鍵更新をおこなうことで更新された鍵により正当な利用者に対しては、サービスを提供し、サービスの可用性及び利用者の利便性を向上させることを目的とする。

【解決手段】 認証用鍵を用いて通信装置 2 0 0 との間で認証処理をおこなう認証処理部 1 9 7 と、上記認証処理部 1 9 7 による認証処理に用いる認証用鍵を通信装置 2 0 が保持していない場合に新たな認証用鍵を生成し、上記通信装置 2 0 0 が保持している場合で上記認証処理部 1 9 7 による通信装置 2 0 0 との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部 1 6 0 とを備え、上記認証処理部 1 9 7 は、上記更新鍵生成部 1 6 0 により生成された新たな認証用鍵を用いて通信装置 2 0 0 との間での認証処理を再度おこなうことを特徴とする。

【選択図】 図 1

特願 2 0 0 3 - 4 3 2 4 4 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 0 1 3]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内 2 丁目 2 番 3 号

氏 名

三菱電機株式会社